

### **Remarks/Arguments**

This application was filed with 23 claims. Claims 1-23 have been rejected. Claims 1 and 20 have been amended to more distinctly point out and claim the subject matter the Applicant regards as their invention. Claims 2, 5 and 14 have been cancelled. New claims 24-26 have been submitted. Thus, claims 1, 3, 4, 6-13, and 15-26 are currently pending in the Application. Reconsideration of the application based on the remaining claims as amended and arguments submitted below is requested. For all the reasons set forth herein, it is respectfully submitted that claims 1, 3, 4, 6-13, and 15-26 are in condition for allowance.

### **Claim Rejections - 35 U.S.C. § 103(a)**

Claim 1 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Maes et al (U.S. Patent No. 6,016,476) in view of U.S. Patent Publication 2003/0149662 A1 to Shore. For all the reasons set forth herein, it is respectfully requested that the rejection of Claim 1 under 35 U.S.C. § 103(a) should be withdrawn.

Claims 1 recites a device having “a magnetic strip that is readable by a standard swipe card reader” and “a biometric sensor for detecting biometric information and producing a sensed biometric profile in a response to a received request for an authentication signal”. Maes is different in that Maes configures a card 26 for use as a selected credit card. The card is then used as the selected credit card. The card 26 does not have a biometric sensor and the PDA 10 does not have a

readable magnetic strip that can interface with a card reader. Thus, neither the card 26 nor the PDA 10 of Maes has both a biometric sensor and a readable magnetic strip. Thus, the device 10 of Maes transfers data to a card reader 30 by configuring a card 26 with the device 10 and then using the card 26 to interface with the card reader 218. Conversely, claim 1 recites a card swipe interface on a device with a biometric sensor. The present invention as recited in claim 1 eliminates the step of configuring the card with the device and then using the card to interface to the card reader and, thus, is an improvement upon Maes. Shore also does not disclose a device biometric sensor with a readable magnetic strip.

Claim 1 has been amended to recite “input communication means including software for receiving a request for an authentication signal from a remote terminal”. The Office Action previously rejected this limitation based upon Maes figure 1 which shows an RF port 50, IR port 54, telephone line interface 46, serial port 42 and parallel port 44. While these are examples of communication means, they do not include “software for receiving a request for an authentication signal from a remote terminal”. The device of Maes merely writes the data to the universal card 26 which is scanned in the reader. This difference between Maes and the present invention is due to the fact that Maes configures a smart card for use as a selected credit card. The smart card is then used as the selected credit card. Conversely, the present invention as recited in claim 1 has a biometric sensor; receives a request for an authentication signal from a remote terminal and responds with an authentication signal.

Regarding claim 3, none of the output communication means disclosed in Maes or Shore are proximity antennas. Such an antenna provides a distinct advantage over the references because it allows the device to be used by simply placing the device in proximity to the reader while not outputting easily interceptable transmissions that are detectable from a long distance. There is also no suggestion in either reference that they would benefit from the use of such an antenna.

Claim 5 is dependent upon claim 1 and therefore allowable for all the reasons stated above with respect to claim 1.

Claim 6 is dependent upon claim 1 and, therefore, allowable for all the reasons stated above with respect to claim 1. In addition, Maes recites a speaker. The card of Maes does not have a speaker and the PDA does not interface with a magnetic strip reader.

With regard to claim 7, Neither Maes nor Shore discloses a device that has a processor that can manipulate information on a magnetic strip on the device. A smart card such as disclosed in Maes uses electrical contacts 30, not a magnetic stripe, on the card to connect with a terminal. The present invention as recited in claim 7 is beneficial in that the electrical device itself can interface with a magnetic stripe reader in an alterable manner.

Claims 8 and 9 are dependent upon claim 1 and, therefore, allowable for all the reasons stated above with respect to claim 1.

With regard to claim 10, the universal card 26 is not the PDA in Maes and the PDA in Maes does not have a protrusion that is adapted to engage a swipe card reader. Rather, Maes uses a removable card to interface with a card reader. The present invention as recited in claim 10 is an electronic device with a processor that has the recited communication means and power supply and “a protrusion that is adapted to engage a swipe card reader”. A clearly different device than that disclosed or suggested in either Maes or Shore.

Regarding claim 11, claim 11 recites an electronic data assistant that has “a card swipe interface that allows stored data to be communicated to a magnetic card reader” and “a processor for comparing said personal identification information and producing an authentication signal based upon said comparison”has a that input that allows said electronic data assistant to receive personal identifying data from a remote source Maes does not disclose an electronic data assistant that has “a card swipe interface that allows stored data to be communicated to a magnetic card reader”; an “input that allows said electronic data assistant to receive personal identifying data from a remote source”; and “a processor for comparing said personal identification information and producing an authentication signal based upon said comparison”. Rather, the device of Mayes transfers data to a card reader 30 by configuring a card 26 with a PDA 10 and then uses the card 26 to interface with the card reader 30. The present invention as recited in claim 11 eliminates the step of configuring the card with the device and then using the card to interface to the card reader and, thus, is an improvement upon Maes and not disclosed in Shore.

Claims 12, 13 and 15 are dependent upon claim 11 and, therefore, allowable for all the reasons stated above with respect to claim 11.

Claim 16 recites an electronic data assistant having a proximity antenna that is not disclosed in either Maes or Shore.

Claims 17 and 18 are dependent upon claim 11 and, therefore, allowable for all the reasons stated above with respect to claim 11.

Claim 18 is dependent upon claim 11 and, therefore, allowable for all the reasons stated above with respect to claim 11.

Claim 19 recites the electronic data assistant of claim 11 wherein “the card swipe interface further comprises a blade-shaped protrusion adapted to be accepted by a card reader”. This feature is totally lacking in any of the cited references.

Claims 20-23 were rejected under 35 USC 103(a) as being unpatentable over U.S. Patent No. 5,917,913 to Wang in view of Maes.

Claim 20 recites a method of authorizing an individual to access an account or perform a transaction. The method involves the steps of detecting a communication center’s request for an identification with a portable electronic device; prompting an individual to respond to said request for an identification by providing biometric information to said portable electronic device; receiving said biometric information from said user; processing said biometric information to determine if said biometric information corresponds to a biometric profile; producing an authentication signal; and communicating said authentication signal

to said communication center in response to receiving said request for an identification.

Wang discloses an electronic authorization device that allows a user to authorize a payment. However, Wang is concerned with encrypting the authorization data in the device itself such that the unencrypted information can not be intercepted. Wang encrypts the identification data and sends it to the remote terminal. The present invention processes the identification data and produces an authentication signal that indicates that the individual holding the card is authorized to make the transaction. Thus, the identification data itself is not encrypted and sent to the remote terminal as in Wang. Maes does not produce an authentication signal in response to a request from a communication center. Maes simply identifies the individual and then writes the information to the universal card.

The present invention as recited in claim 20 insures that the data is in the possession of the individual that is authorized to have the device by comparing the sensed biometric information to a biometric profile stored on the device and then producing an authentication signal. However, the biometrically identifying information itself resides only on the device and is not accessible to, or transmitted to, the remote terminal. This helps protect the individual from having digital versions of their biometric data stolen and reduces the need to encrypt the data. Conversely, in Maes, the biometric identifying information is stored on the PDA where it can be accessed from a central server as described in the specification and

transferred to the card where it may be read or stolen. Neither, Maes nor Shore discloses validating the biometric data with the device, producing an authentication signal which is sent to the remote terminal and transmitting the authentication signal to the remote terminal in a manner that prevents the remote terminal from accessing the biometric data.

The fact that an authentication signal is produced to verify the user and it is the authentication signal that is sent to the remote terminal in response to the communication center's request distinguishes the present invention from Maes.

Claims 21-23 are dependent upon claim 20 and therefore allowable for all the reasons stated above with respect to claim 20.

New claim 24 depends from claim 1 and further recites that "said device performs an initial verification of a user's identity prior to transmitting any data to an external device". Maes immediately contacts a communication server. FIG. 4, 100. This initial communication provides an opportunity for hacking into the device. By verifying a user's identity prior to transmitting any data, the present invention as recited in new claim 24 improves upon the cited prior art.


New claim 25 recites the portable device of claim 1 further comprising tamper resistant hardware or software that detects attempts to access data stored on the device or access a restricted portion of the device and erases stored data based upon the detection. Maes does not mention or suggest such a feature.

Newly submitted claim 26 recites the device of claim 1 wherein an identity of the remote terminal is verified to ensure that the remote terminal's is a known or

authorized source. This insures that that the device is not being spoofed or hacked into. Maes does not verify the communication server and does not disclose such a feature.

Applicant has commented on some of the distinctions between the cited references and the claims to facilitate a better understanding of the present invention. This discussion is not exhaustive with regard to all of the features of the invention, and Applicant hereby reserves the right to present additional distinctions as appropriate. Furthermore, while these remarks may employ shortened, more specific, or variant descriptions of some of the claim language, Applicant respectfully notes that these remarks are not to be used to create implied limitations in the claims and only the actual wording of the claims should be considered against these references.

Respectfully submitted,



---

Jason L. Hornkohl  
Registration No. 44,777  
Hornkohl Law Firm

ATTORNEY FOR APPLICANT

Jason L. Hornkohl  
Hornkohl Law Firm  
P.O. Box 210584  
Nashville, TN 37221  
(615) 673-6771



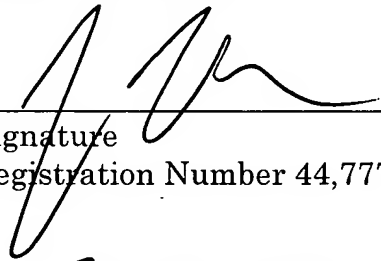
## CERTIFICATE OF FIRST CLASS MAILING

I hereby certify that this Response and Amendment in Application Serial No. 10/628,282 having a filing date of July 25, 2003 is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

on March 22, 2007.

Jason L. Hornkohl



---

Signature  
Registration Number 44,777

3-22-07  
Date